Chapter 12
Critical Nodes Detection in IoT-Based Cyber-Physical Systems: Applications, Methods, and Challenges

Onur Ugurlu
Izmir Bakircay University, Turkey

Nusin Akram
Ege University, Turkey

Vahid Khalilpour Akram
Ege University, Turkey

ABSTRACT

The new generation of fast, small, and energy-efficient devices that can connect to the internet are already used for different purposes in healthcare, smart homes, smart cities, industrial automation, and entertainment. One of the main requirements in all kinds of cyber-physical systems is a reliable communication platform. In a wired or wireless network, losing some special nodes may disconnect the communication paths between other nodes. Generally, these nodes, which are called critical nodes, have many undesired effects on the network. The authors focus on three different problems. The first problem is finding the nodes whose removal minimizes the pairwise connectivity in the residual network. The second problem is finding the nodes whose removal maximizes the number of connected components. Finally, the third problem is finding the nodes whose removal minimizes the size of the largest connected component. All three problems are NP-Complete, and the authors provide a brief survey about the existing approximated algorithms for these problems.

INTRODUCTION

Internet of Things (IoT) is one the fastest growing and most promising technologies that already have influenced the daily life of most people in different areas. Especially with the emerging of smartphones,

DOI: 10.4018/978-1-7998-4186-9.ch012

people can easily connect to remote devices and control them using their phones. Intelligent homes that automatically control temperature, lights, doors, security, and entertainment facilities is an example of IoT based systems (Zielonka, 2020). The number and diversity of furniture that connects to the internet are growing day by day. Most of the recently produced refrigerators, washing machines, coffeemakers, sound systems, televisions, air conditioning systems, and dishwashers allow their users to control them over the Internet or local network. Intelligent greenhouses (Castañeda-Miranda, 2020), autonomous vehicles (Minovski, 2020), smart manufacturing systems (Tran, 2021), intelligent transportation systems (Lin, 2020), and indoor or outdoor tracking systems (Adardour, 2021) are some other applications areas of IoT.

The recent advances in hardware and electronic technologies have led to the production of small, fast, and energy-efficient devices that can store a large amount of data, precisely sense different events, perform heavy computation, and communicate over different channels such as WiFi, Bluetooth, and 5G technologies. Generally, these devices may run embedded programs to complete the given tasks. They support different communication ports so the users can use them inside other smart things or directly connect them over available ports. The available devices for IoT may connect to the Internet over cabled networks, wireless networks, or multi-hop networks. In this way, we may establish IoT networks almost everywhere, even in harsh environments such as forests or mountains.

One of the most essential requirements in IoT-based systems is communication. Generally, IoT-based systems consist of many different nodes for various tasks such as sensing the events or quantities, processing the gathered data, storing the information, and performing some mechanical tasks such as opening a door or rotating a valve. Most of these tasks are completed by remote nodes which are controlled over the Internet or a communication platform. Based on the application type and available infrastructure, different platforms can be used for establishing the connection between the nodes or end-users. For example, in intelligent home controlling systems, the IoT nodes can connect to the Internet over a local area network or WiFi platform. In a public transportation system or in an outdoor tracking system (for example, tracking cargo packets), the nodes may use 4G or 5G cellular network to communicate with the controlling center. In this way, the users may track the real-time location of the next bus or their cargo. As another example, in a forest fire controlling system, the nodes may use multi-hop ad-hoc connections to cover a wide area and send their gathered data to the controlling center. In this system, each node should send its collected data to the next node until they reach the base station which is connected to the Internet.

Regardless of the type of communication platform, generally, most IoT-based applications need continuous, secure, and fault tolerance communication channels to send their data or receive new commands from the remote nodes. While losing the connection to some nodes for a limited time can be tolerated in some applications (for example, in a forest fire control system), a strict and real-time connection is required in many other applications (for example, in military operations). However, almost all communication platforms may fail due to different hardware problems, software errors, or environmental conditions. The WiFi network may go off because of temporal electric failures. A 5G base station may stop working because of environmental conditions such as a storm. In a multi-hop wireless sensor network, some nodes may stop working because of battery drain. Hence, most IoT-based systems must increase the robustness of the connections as much as possible and should have accurate plans for failure scenarios to improve the reliability of the systems.

Finding the weak points or critical parts of a system is the first step for increasing the system's reliability. In a communication network, failure of a critical node (for example, a router or a node that forwards most of the traffic) or weak communication links (for example, a link with a high error ratio) may disconnect the communication path between the base station and remote nodes. This is an undesirable